What is claimed is:

1. A method for establishing an authenticated wireless communication between a first mobile device and a second device, comprising the steps of:

sending an initial signal by the first device to establish a wireless communication with the second device, the first device including only a data capturing arrangement ("DCA") as an input device interface with a user thereof;

initiating an authentication process by the second device;

obtaining the PIN code from the user via the DCA;

performing a pairing process to compare the PIN code to entries in a database of authorized PIN codes;

when the pairing process has been successfully completed, generating a link key to establish the authenticated wireless communication between the first and second devices.

2. The method according to claim 1, wherein the databases is stored in a memory arrangement of the second device.

3. The method according to claim 1, wherein the first device is a mobile barcode scanner.

4. The method according to claim 1, wherein the first device communicates with the second device using Bluetooth technology.

5. The method according to claim 1, wherein the obtaining step further includes the following substeps:

scanning a barcode using the DCA, the barcode being provided by the user as the PIN code, and

converting the barcode into the PIN code using a processor of the first device.

6. The method according to claim 1, wherein the second device includes a wireless access point which communicates with the first device.

7. The method according to claim 1, wherein the first device includes an alerting arrangement notifying the user when to enter the PIN code.

8. The method according to claim 7, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a predetermined lighting pattern.

9. The method according to claim 1, wherein the obtaining step includes the following substeps:

limiting a time period for the user to enter the PIN code to a predetermined time period, and

refusing to accept the PIN code from the user when the predetermined time period has expired.

10. The method according to claim 1, wherein the pairing process includes the following substeps:

providing first sample data by the second device to the first device,

generating second data, by the first device, as a

function of the first sample data, the PIN code and a hashing procedure;

providing at least a portion of the second data to the second device,

generating third data by the second device as a function of one of the authorized PIN codes stored in the database, the second data and the hashing procedure;

comparing the second data to the corresponding third data by the second device, and

when the second data matches to the third data, generating an indication the pairing process is successfully completed.

11. The method according to claim 1, wherein the link key is one of a temporary key which is effective only for a single session and a long-term key which is effective for multiple sessions between the first and second devices.

12. The method according to claim 1, further comprising the step of:

establishing a secure communication between the first and second devices using a predetermined encryption technology.

13. A system for establishing an authenticated wireless communication, comprising:

a first wireless mobile device including only a data capturing arrangement ("DCA") as an input device interface with a user thereof; and

a second device receiving an initial signal from the first device to establish a wireless communication, the second

device initiating an authentication process,

wherein the first device obtains the PIN code from the user via the DCA, wherein the first and second devices perform a pairing process to compare the PIN code to entries in a database of authorized PIN codes, and wherein, when the pairing process has been successfully completed, the first and second devices generate a link key to establish the authenticated wireless communication.

14. The system according to claim 13, wherein the second device includes a memory arrangement storing the database.

15. The system according to claim 13, wherein the first device is a mobile barcode scanner.

16. The system according to claim 13, wherein the first device communicates with the second device using Bluetooth technology.

17. The system according to claim 13, wherein the first device scans a barcode using the DCA, the barcode being provided by the user as the PIN code, a processor of the first device converting the barcode into the PIN code.

18. The system according to claim 13, wherein the second device includes a wireless access point which communicates with the first device.

19. The system according to claim 13, wherein the first device includes an alerting arrangement notifying the user to

enter the PIN code.

20. The system according to claim 19, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a light in a predetermined lighting patterns.

21. The system according to claim 13, wherein the pairing process includes the following substeps:

providing first sample data by the second device to the first device;

generating second data, by the first device, as a function of the first sample data, the PIN code and a hashing procedure;

providing at least a portion of the second data to the second device;

generating third data by the second device as a function of one of the authorized PIN codes stored in the database, the second data and the hashing procedure;

comparing the second data to the corresponding third data by the second device; and

when the second data matches to the third data, generating an indication the pairing process is successfully completed.

22. The system according to claim 15, wherein the link key is one of a temporary key which is effective only for a single session and a long-term key which is effective for multiple sessions between the first and second devices.

23. The system according to claim 13, wherein the first and second devices establish a secure communication using a predetermined encryption technology.

24. A wireless mobile device for establishing an authenticated wireless communication with a further device, comprising:

a processor;

a wireless communication arrangement; and

a data capturing arrangement ("DCA") being the only input device interface for a user thereof,

wherein the processor generates a request for establishing an authenticated wireless communication, the request being forwarded to the further device via the communication arrangement, the communication arrangement receives from the further device first data and a request for second data, the DCA obtaining the PIN code from the user, the processor generating the second data as a function of the PIN code, the first data and the hashing procedure, the second data being provided to the further device,

wherein the further device generates third data as a function of one of the authorized PIN codes stored in a database, the second data and the hashing procedure, and

wherein, when the second data matched to the third data, the device and the further device generate a link key to establish the authenticated wireless communication.

25. The device according to claim 24, wherein the device is a mobile barcode scanner.

26. The device according to claim 24, wherein the device communicates with the further device using Bluetooth technology.

27. The device according to claim 24, wherein the DCA scans a barcode which is provided by the user as the PIN code, the processor converting the barcode into the PIN code.

28. The device according to claim 24, further comprising:

an alerting arrangement notifying the user to enter the PIN code.

29. The device according to claim 24, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a predetermined lighting pattern.